Microsoft Security

# SC-900T00-A Module 2: Describe the Capabilities of Microsoft Identity and Access Management Solutions

© Copyright Microsoft Corporation. All rights reserved.

# Module Agenda

- Explore the services and identity types of Azure Active Directory
- Explore the authentication capabilities of Azure Active Directory
- Explore the access management capabilities of Azure Active Directory
- Describe identity protection governance capabilities of Azure Active Directory

© Copyright Microsoft Corporation. All rights reserved.

# Lesson 1: Explore the services and identity types in Azure Active Directory

© Copyright Microsoft Corporation. All rights reserved.

# Lesson 1 Introduction

**After completing this module, you'll be able to:**

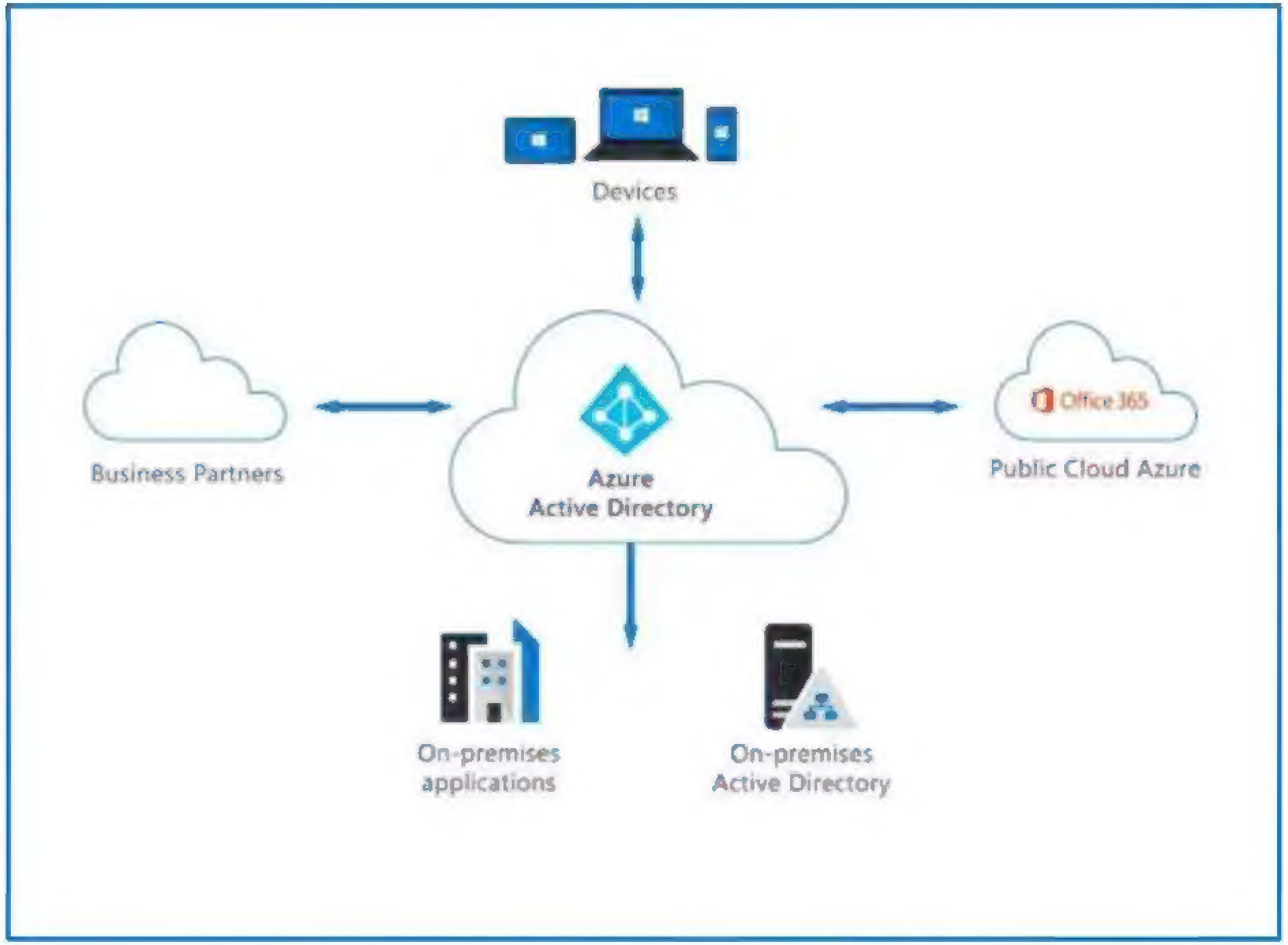
- Describe what is Azure AD
- Describe the identity types that Azure AD supports

© Copyright Microsoft Corporation. All rights reserved.

# Azure Active Directory

**Azure AD is Microsoft's cloud-based identity and access management service. Capabilities of Azure AD include:**

- Organizations can enable their employees, guests, and others to sign in and access the resources they need.
- Provide a single identity system for their cloud and on-premises applications.
- Protect user identities and credentials and to meet an organization's access governance requirements.
- Each Microsoft 365, Office 365, Azure, and Dynamics 365 Online subscription automatically use an Azure AD tenant.



© Copyright Microsoft Corporation. All rights reserved.

# Azure AD identity types

Azure AD manages different types of identities: users, service principals, managed identities, and devices.

**User** – Generally speaking, a user is a representation of an individual's identity that's managed by Azure AD. Employees and guests are represented as users in Azure AD.

**Device** - A piece of hardware, such as mobile devices, laptops, servers, or printer. Device identities can be set up in different ways in Azure AD, to determine properties such as who owns the device.

**Service principal** - You can think of it as an identity for an application. A service principal is created in every tenant the application is used & defines who can access the app, what resources the app can access, and more.

**Managed identity** – A type of service principal, a managed identity provides an identity for applications to use when connecting to resources that support Azure AD authentication.

© Copyright Microsoft Corporation. All rights reserved.

Microsoft Security

# Demo

## Azure Active Directory user settings

© Copyright Microsoft Corporation. All rights reserved.

# External identities in Azure AD

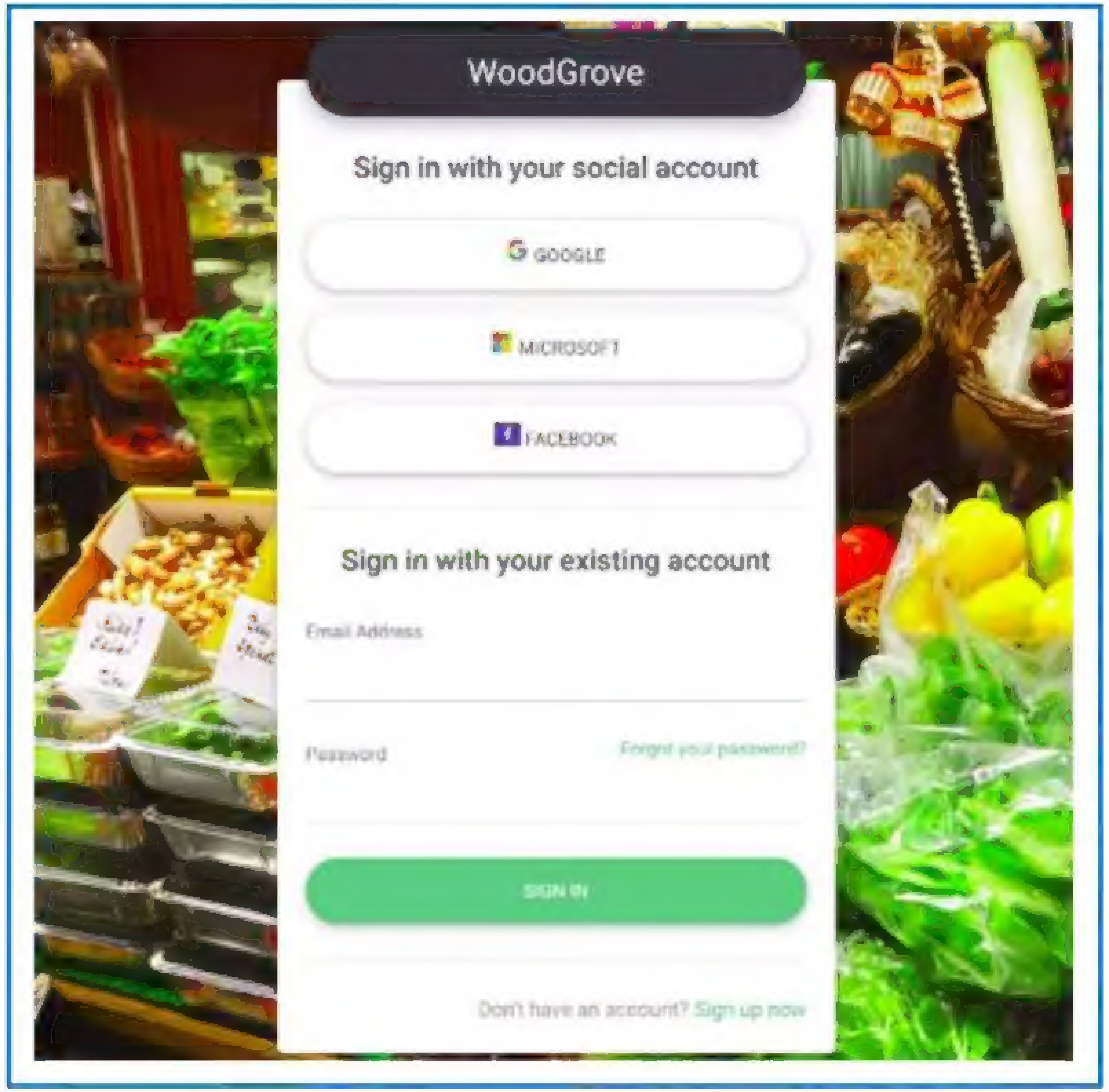
**Two different Azure AD External Identities:**

### B2B collaboration

B2B collaboration allows you to share your apps and resources with external users

### B2C access management

B2C is an identity management solution for consumer and customer facing apps


WoodGrove
Sign in with your social account
GOOGLE
MICROSOFT
FACEBOOK
Sign in with your existing account
Email Address
Password
Forgot your password?
SIGN IN
Don't have an account? Sign up now

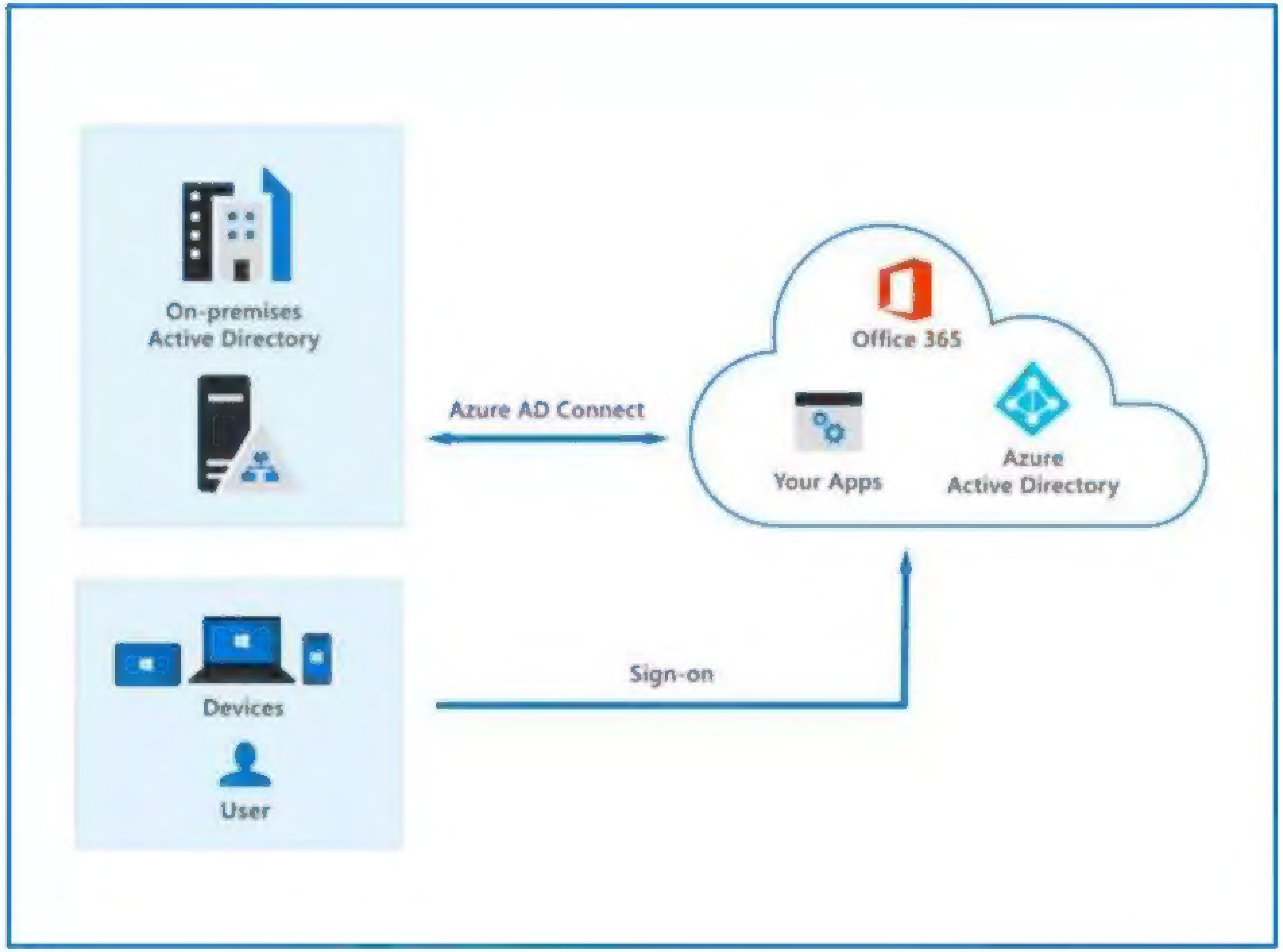
© Copyright Microsoft Corporation. All rights reserved.

# The concept of hybrid identities

## Hybrid identities

### Hybrid identity model

- With the hybrid model, users accessing both on-premises and cloud apps are hybrid users managed in the on-premises Active Directory.
- When you make an update in your on-premises AD DS, all updates to user accounts, groups, and contacts are synchronized to your Azure AD with ***Azure AD Connect***



© Copyright Microsoft Corporation. All rights reserved.

# Lesson 2: Explore the authentication capabilities of Azure Active Directory

© Copyright Microsoft Corporation. All rights reserved.

# Lesson 2 Introduction

**After completing this module, you'll be able to:**

- Describe the secure authentication methods of Azure AD
- Describe the password protection and management capabilities of Azure AD

© Copyright Microsoft Corporation. All rights reserved.

# Authentication methods of Azure AD

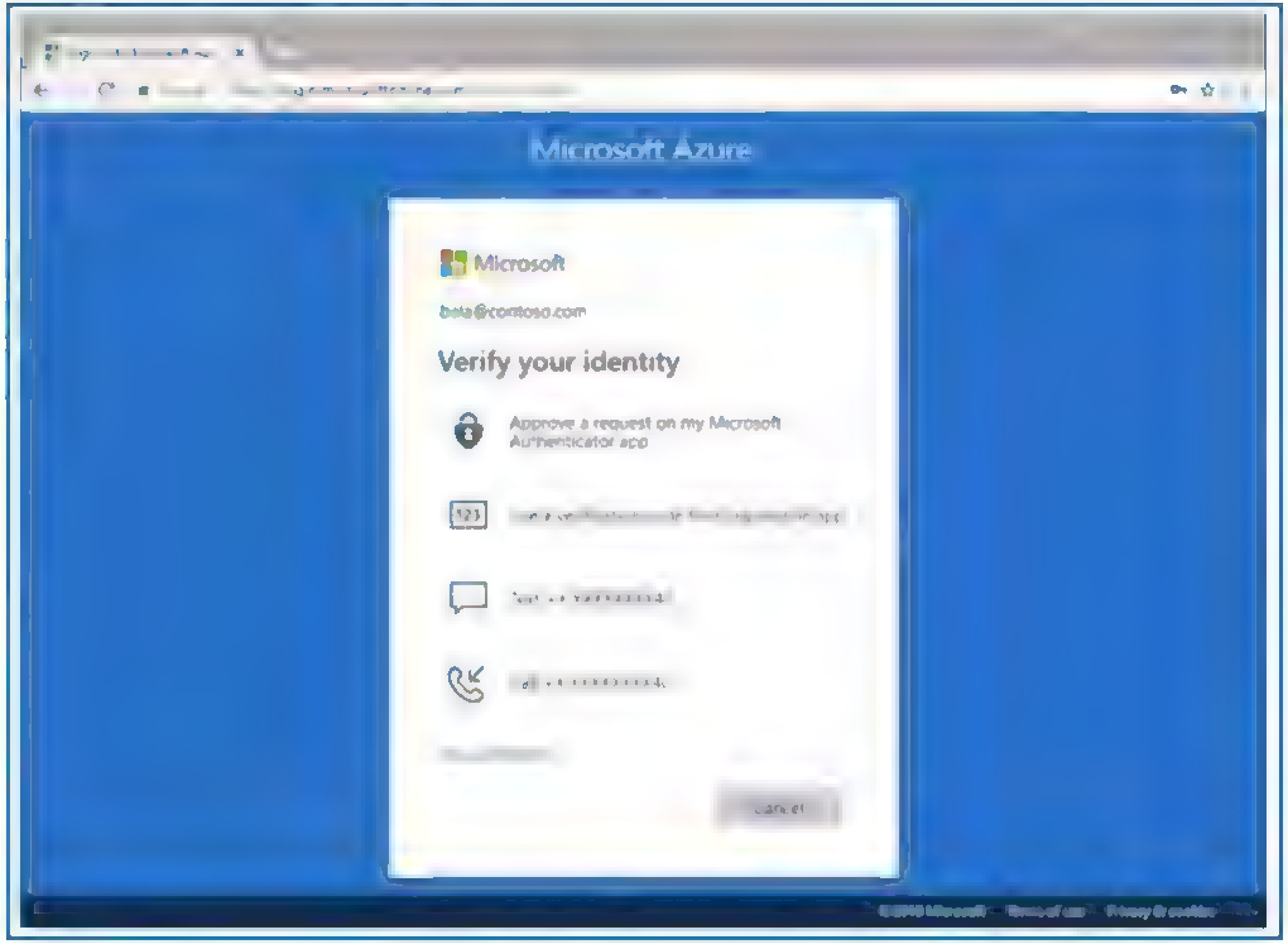
## Multifactor authentication (MFA) & Security Defaults

### MFA requires more than one form of verification:

- Something you know
- Something you have
- Something you are

### Security defaults:

- A set of basic identity security mechanisms recommended by Microsoft.
- A great option for organizations that want to increase their security posture but don't know where to start, or for organizations using the free tier of Azure AD licensing.



Microsoft Azure

Microsoft

bala@contoso.com

Verify your identity

Approve a request on my Microsoft Authenticator app

© Copyright Microsoft Corporation. All rights reserved.

# Multi-factor authentication (MFA) in Azure AD

## Different authentication methods that can be used with MFA

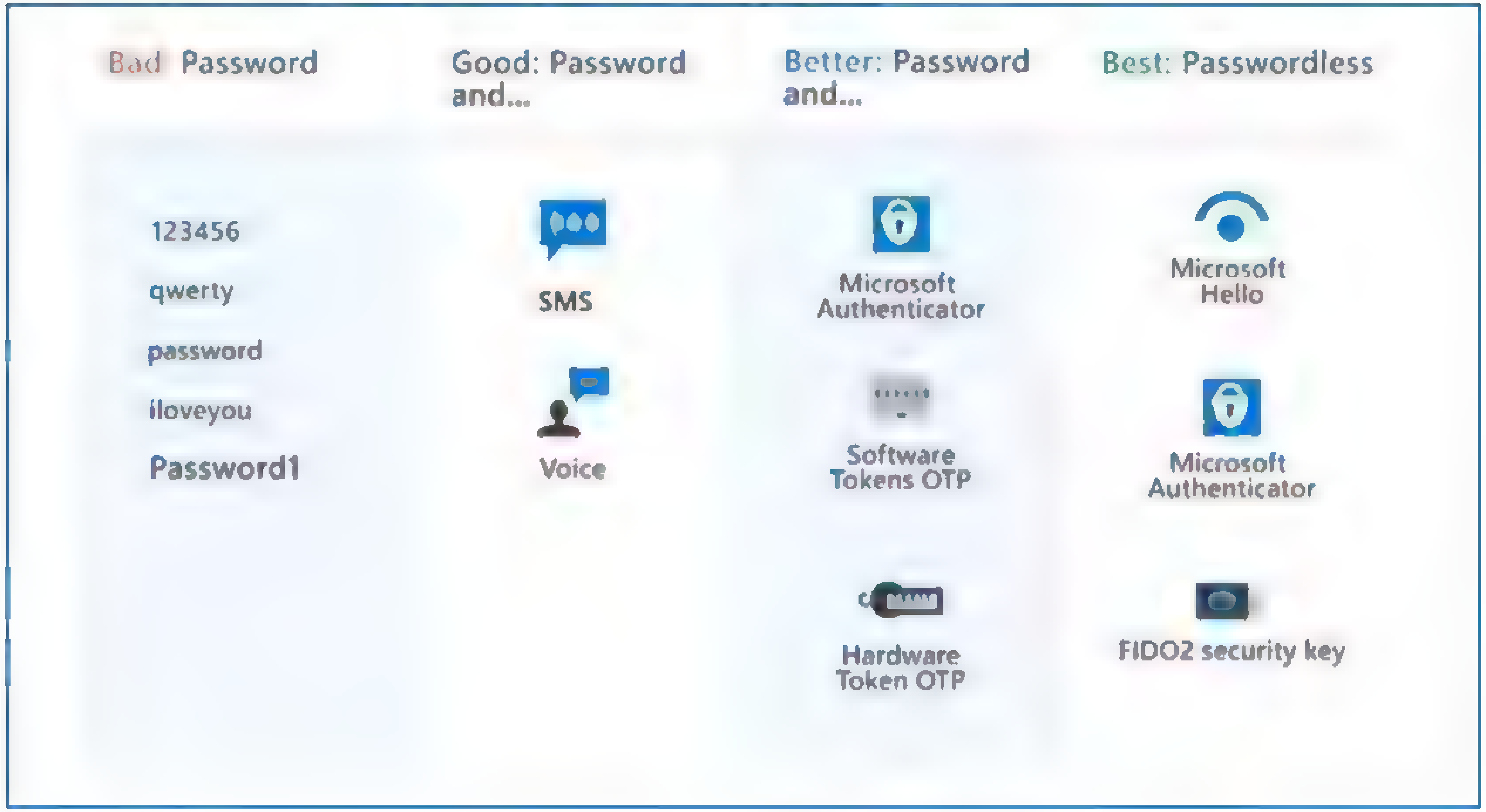
Passwords

Password & additional verification

- Phone (voice or SMS)
- Microsoft Authenticator
- Open Authentication (OATH) with software or hardware tokens

Passwordless

- Biometrics (Windows Hello)
- Microsoft Authenticator
- FIDO2



| Bad Password | Good: Password and... | Better: Password and... | Best: Passwordless |
|---|---|---|---|
| 123456<br>qwerty<br>password<br>iloveyou<br>Password1 | SMS<br>Voice | Microsoft Authenticator<br>Software Tokens OTP<br>Hardware Token OTP | Microsoft Hello<br>Microsoft Authenticator<br>FIDO2 security key |

© Copyright Microsoft Corporation. All rights reserved.

# Windows Hello for Business

## Windows Hello lets users authenticate to:

- A Microsoft account
- An Active Directory account
- An Azure Active Directory (Azure AD) account
- Identity Provider Services or Relying Party Services that support Fast ID Online v2.0 authentication

## Why is Windows Hello safer than a password?

Because it's tied to the specific device on which it was set up. Without the hardware, the PIN is useless

© Copyright Microsoft Corporation. All rights reserved.

# Self-service password reset (SSPR) in Azure AD

## Benefits of Self-service password reset:

- It increases security.
- It saves the organization money by reducing the number of calls and requests to help desk staff.
- It increases productivity, allowing the user to return to work faster.

## Self-service password reset works in the following scenarios:

- Password change
- Password reset
- Account unlock

## Authentication method of SSPR:

- Mobile app notification
- Mobile app code
- Email

© Copyright Microsoft Corporation. All rights reserved.

Microsoft Security

# Demo

## Azure Active Directory self-service password reset (SSPR)

© Copyright Microsoft Corporation. All rights reserved

# Password protection & management capabilities in Azure AD

- Global banned password list
- Custom banned password lists
- Protecting against password spray
- Hybrid security

© Copyright Microsoft Corporation. All rights reserved.

# Lesson 3: Explore the access management capabilities of Azure Active Directory

© Copyright Microsoft Corporation. All rights reserved.

# Lesson 3 Introduction

**After completing this module, you'll be able to:**

- Describe Conditional Access and its benefits
- Describe Azure AD roles

© Copyright Microsoft Corporation. All rights reserved.

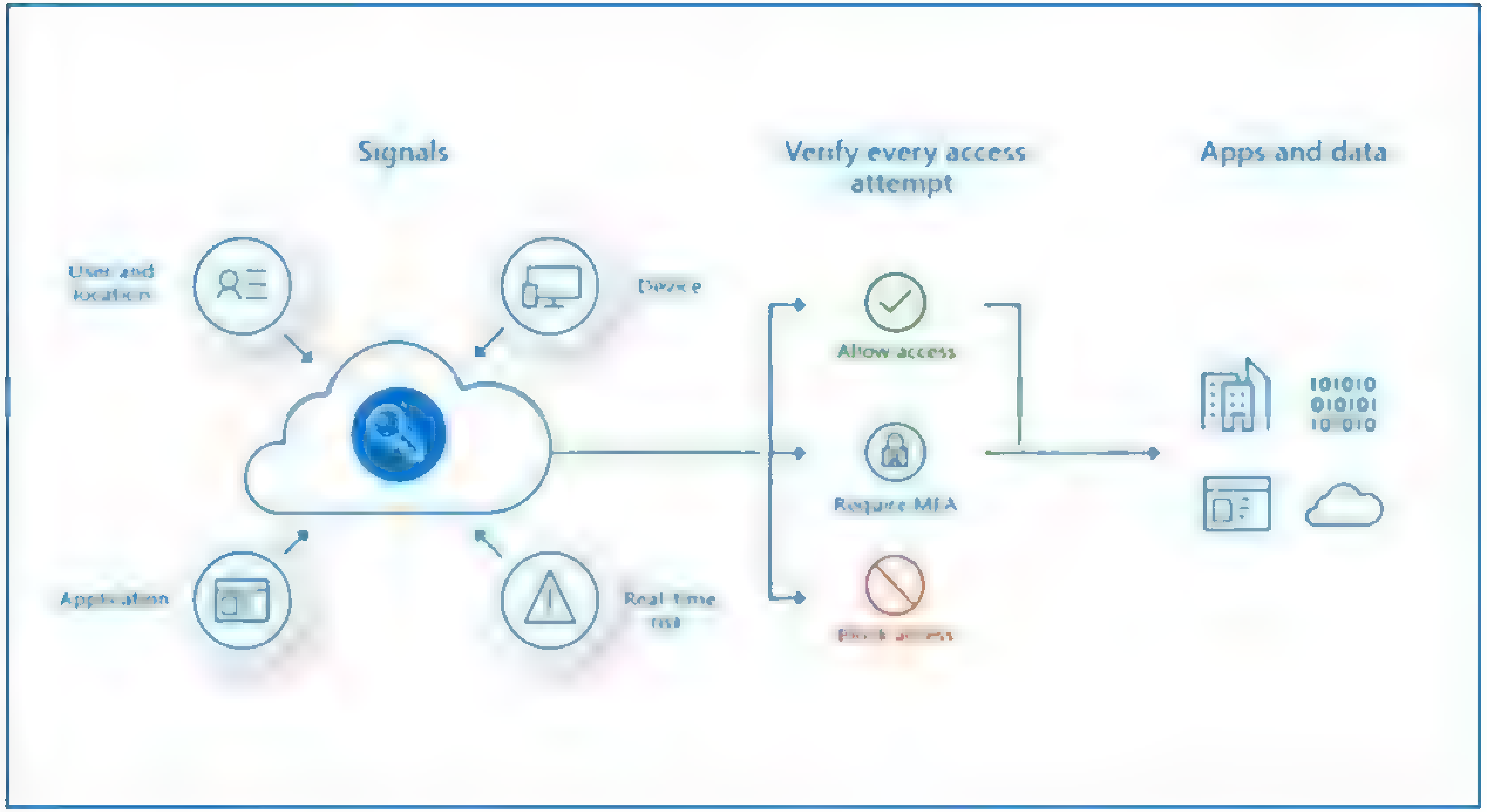
# Conditional access

**Conditional Access signals:**

- User or group membership
- Named location information
- Device
- Application
- Real-time sign-in risk detection
- Cloud apps or actions
- User risk

**Access controls:**

- Block access
- Grant access
- Require one or more conditions to be met before granting access
- Control user access based on session controls to enable limited experiences within specific cloud applications



© Copyright Microsoft Corporation. All rights reserved.

Microsoft Security

# Demo

## Azure Active Directory Conditional Access

© Copyright Microsoft Corporation. All rights reserved.

# Azure AD role-based access control (RBAC)

Azure AD roles control permissions to manage Azure AD resources.

- Built-in roles
- Custom roles
- Azure AD role-based access control
- Only grant the access users need

© Copyright Microsoft Corporation. All rights reserved.

# Lesson 4: Describe the identity protection and governance capabilities of Azure Active Directory

© Copyright Microsoft Corporation. All rights reserved.

# Lesson 4 Introduction

**After completing this module, you'll be able to:**

- Describe the identity governance capabilities of Azure AD.
- Describe the benefits of Privileged Identity Management (PIM).
- Describe the capabilities of Azure AD Identity Protection.

© Copyright Microsoft Corporation. All rights reserved.

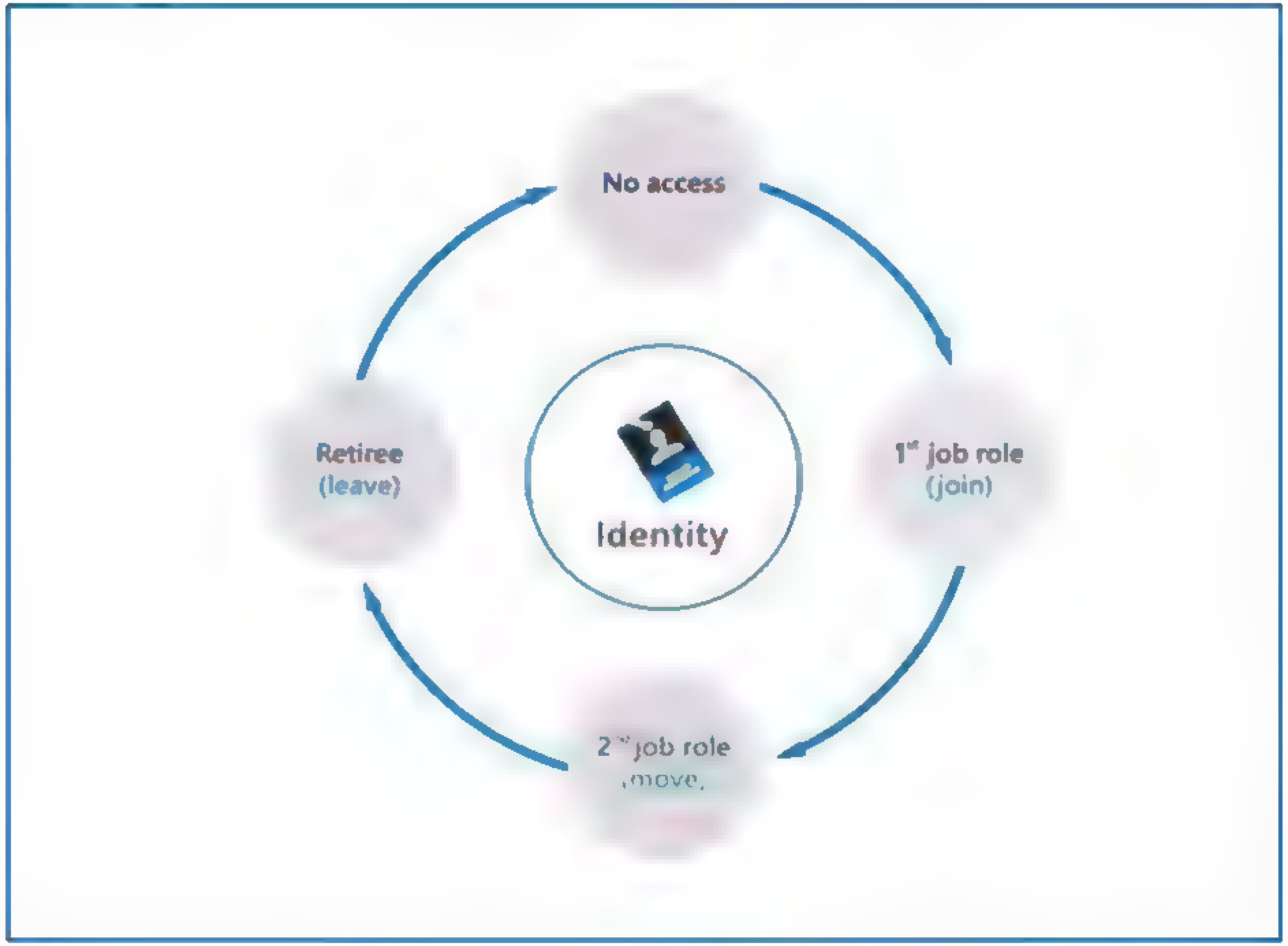
# Identity governance in Azure AD

### The tasks of Azure AD identity governance

- Govern the identity lifecycle.
- Govern access lifecycle.
- Secure privileged access for administration.

### Identity lifecycle

- Join:  A new digital identity is created.
- Move:  Update access authorizations.
- Leave:  Access may need to be removed.



© Copyright Microsoft Corporation. All rights reserved.

# Entitlement management and access reviews

## Entitlement management

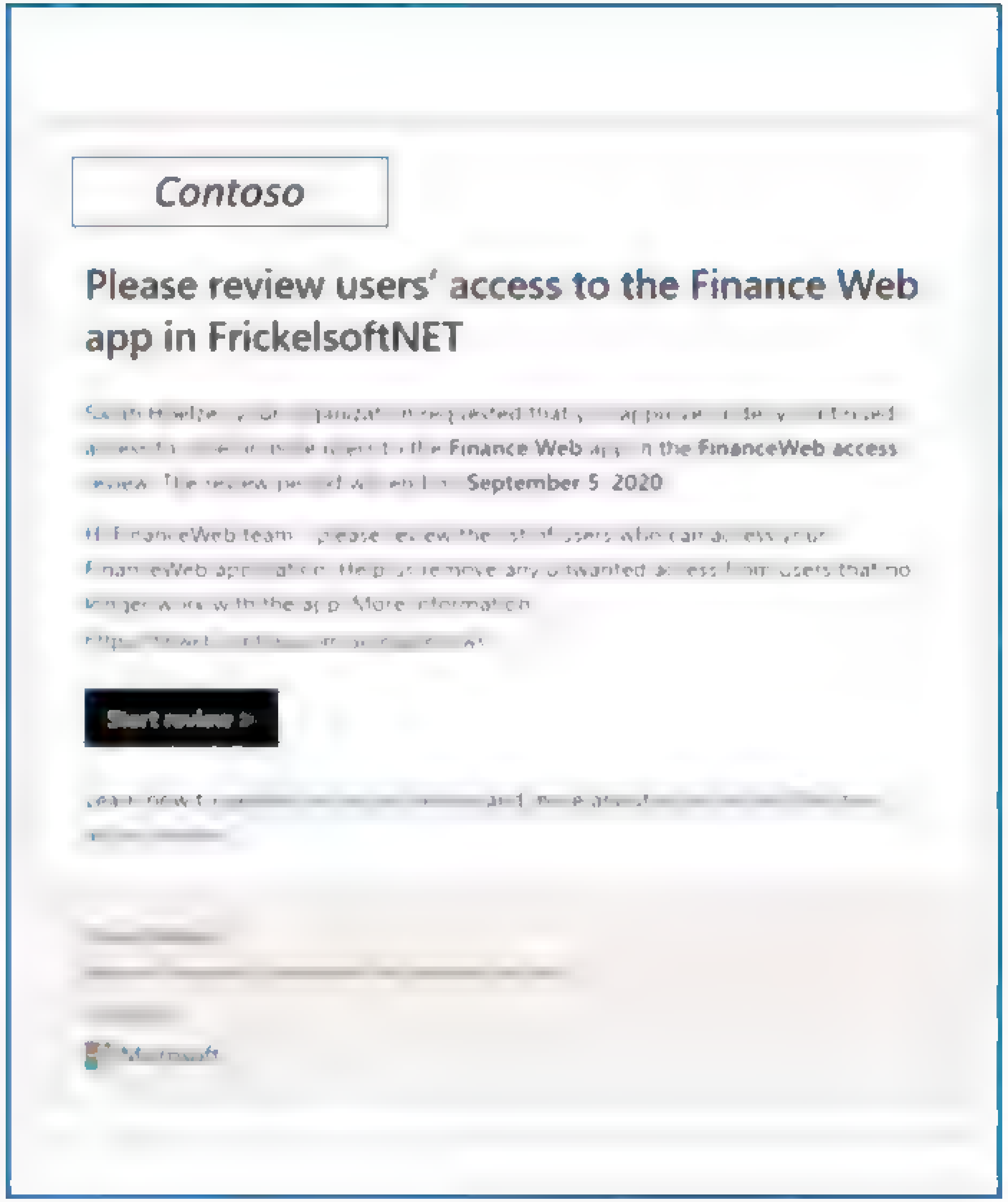
- It is an identity governance feature that enables organizations to manage identity and access lifecycle at scale.
- It automates access request workflows, access assignments, reviews, and expiration.

## Access reviews

- Enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignment.
- Ensure that only the right people have access to resources
- Used to review and manage access for both users and guests

## Terms of use

- Allow information to be presented to users, before they access data or an application.
- Ensure users read relevant disclaimers for legal or compliance requirements.



Contoso

**Please review users' access to the Finance Web app in FrickelsoftNET**

© Copyright Microsoft Corporation. All rights reserved.

# Privileged Identity Management (PIM)

PIM enables you to manage, control, and monitor access to important resources in your organization.

- Just in time, providing privileged access only when needed, and not before.
- Time-bound, by assigning start and end dates that indicate when a user can access resources.
- Approval-based, requiring specific approval to activate privileges.
- Visible, sending notifications when privileged roles are activated.
- Auditable, allowing a full access history to be downloaded.

© Copyright Microsoft Corporation. All rights reserved.

# Azure Identity Protection

Enables organizations to accomplish three key tasks:

- Automate the detection and remediation of identity-based risks.
- Investigate risks using data in the portal.
- Export risk detection data to third-party utilities for further analysis.

It can categorize and calculate risk:

- Categorize risk into three tiers: low, medium, and high.
- Calculate the sign-in risk, and user identity risk.

It provides organizations with three reports:

- Risky users
- Risky sign-ins
- Risk detections

© Copyright Microsoft Corporation. All rights reserved.

# Module Summary

**In this module, you have:**

- Learned about Azure AD and services and identity types Azure AD supports
- Explore the authentication capabilities of Azure AD, including MFA
- Explore the access management capabilities of Azure AD with Conditional Access and Azure AD RBAC
- Describe identity protection and governance capabilities of Azure AD, including PIM, entitlement management, and access reviews.
- Learned about the capabilities of Azure AD Identity Protection.

© Copyright Microsoft Corporation. All rights reserved.

Microsoft Security

© Copyright Microsoft Corporation. All rights reserved.